Amendments to the Claims

1-21. (cancelled)

22. (original) A method of downloading data to an MPEG receiver/decoder, comprising the steps of:

generating a signature for the data to be downloaded;

including the signature and other data in a block of data with a selected offset between the start of the data block and the start of the signature;

encrypting the data block using a private key;

formatting the data to be downloaded and the encrypted data block as an MPEG table;

transmitting the MPEG table; and

at the receiver/decoder:

receiving the MPEG table;

decrypting the encrypted data block in the received MPEG table using a public key corresponding to the private key;

looking up at least one stored offset in a protected area of memory of the receiver/decoder;

extracting the signature from the decrypted data block using said one looked-up offset from the start of the decrypted data block;

generating a signature for the data in the received MPEG table; and

comparing the signature extracted from the decrypted data block with the signature generated at the receiver/decoder for the received data.

23. (amended) A method as claimed in claim ~~21~~ 22, wherein said protected area of memory has at least two such stored offsets, and, if in the comparing step the extracted signature and the generated signature do not match, further including the steps of repeating the looking-up, extracting and comparing steps using another of the stored offsets.

24. (amended) A method as claimed in claim ~~21~~ 22, wherein at least some of said other data in the block of data is dummy or arbitrary data.

25. (amended) A method as claimed in claim ~~11~~ 22, wherein the data is downloaded as a plurality of modules of the data, and including the steps of:

generating a module signature for each module of data to be downloaded;

formatting the modules of data as respective module MPEG tables;

generating a directory including an identification of each module MPEG table and the respective signature, the directory being the subject of the signature generating step; and

at the receiver/decoder:

generating a respective module signature for each of the modules in the received module MPEG tables; and

comparing each module signature in the received directory MPEG table with the respective module signature generated at the receiver/decoder.

26. (cancelled)

27. (previously amended) A method as claimed in claim 25, further including the step of inhibiting or aborting downloading of such a module of the data if, in the module signature comparing step, the module signature in the received directory MPEG table and the respective module signature generated at the receiver/decoder for that module do not match each other.

28. (amended) A method as claimed in claim ~~11~~ 22, further including the step of inhibiting or aborting downloading of the data if, in the comparing step(s), the or each decrypted signature and the generated signature do not match each other.

29-46. (cancelled)

47. (amended) An MPEG receiver/decoder ~~for use in performing part of the method of claim 22,~~ comprising:

means for receiving ~~such~~ MPEG tables, wherein each MPEG table includes a signature and other data in a block of data with a selected offset between the start of the data block and the start of the signature, wherein the block of data is encrypted using a private key;

means for storing a public key and an identification for the public key;

a protected area of memory for storing at least one offset; and

processing means ~~which is~~ programmed to decrypt the encrypted data block in such a received MPEG table using the stored public key corresponding to the private key; to look-up said one stored offset in the protected area of memory; to extract the signature from the decrypted data block using the looked-up offset from the start of the

decrypted data block; to generate a signature for the data in the received MPEG table; and to compare the signature extracted from the decrypted data block with the signature generated at the receiver/decoder for the received data.

48. (amended) A receiver/decoder as claimed in claim ~~46~~ 47, wherein at least two such offsets are stored in the protected area of the memory, and the processing means is operable, if the extracted signature and the generated signature do not match, to repeat the looking-up, extracting and comparing using another of the stored offsets.

49. (amended) A received/decoder as claimed in claim ~~46~~ 47, wherein the memory for storing the offset is provided by rewritable non-volatile memory.

50. (amended) A receiver/decoder as claimed in claim ~~29~~ 47, wherein the processing means is programmed to generate a respective module signature for each of the modules in the received module MPEG tables, and to compare each module signature in the received ~~directory~~ MPEG table with the respective module signature generated by the receiver/decoder.

51. (cancelled)

52. (previously amended) A receiver/decoder as claimed in claim 50, wherein the processing means is programmed to inhibit or abort downloading of such a module of the data if the module signature in the received ~~directory~~ MPEG table and the respective

module signature generated at the receiver/decoder for that module do not match each other.

53. (amended) A receiver/decoder as claimed in claim ~~29~~ 47, wherein the processing means is programmed to inhibit or abort downloading of the data if the or each decrypted signature and the generated signature do not match each other.

54-56. (cancelled)

57. (new) An MPEG receiver/decoder comprising:

a receiver configured to receive an MPEG table from a transmitter, wherein the MPEG table includes a signature and other data in a block of data with a selected offset between the start of the data block and the start of the signature, wherein the block of data is encrypted using a private key;

a memory for storing a public key corresponding to the private key; and

a processor programmed to

decrypt the encrypted data block in the received MPEG table using the public key,

look-up at least one stored offset in the memory,

extract the signature from the decrypted data block using the looked-up offset,

generate a signature for the data in the received MPEG table, and

compare the signature extracted from the decrypted data block with the signature generated at the receiver/decoder.